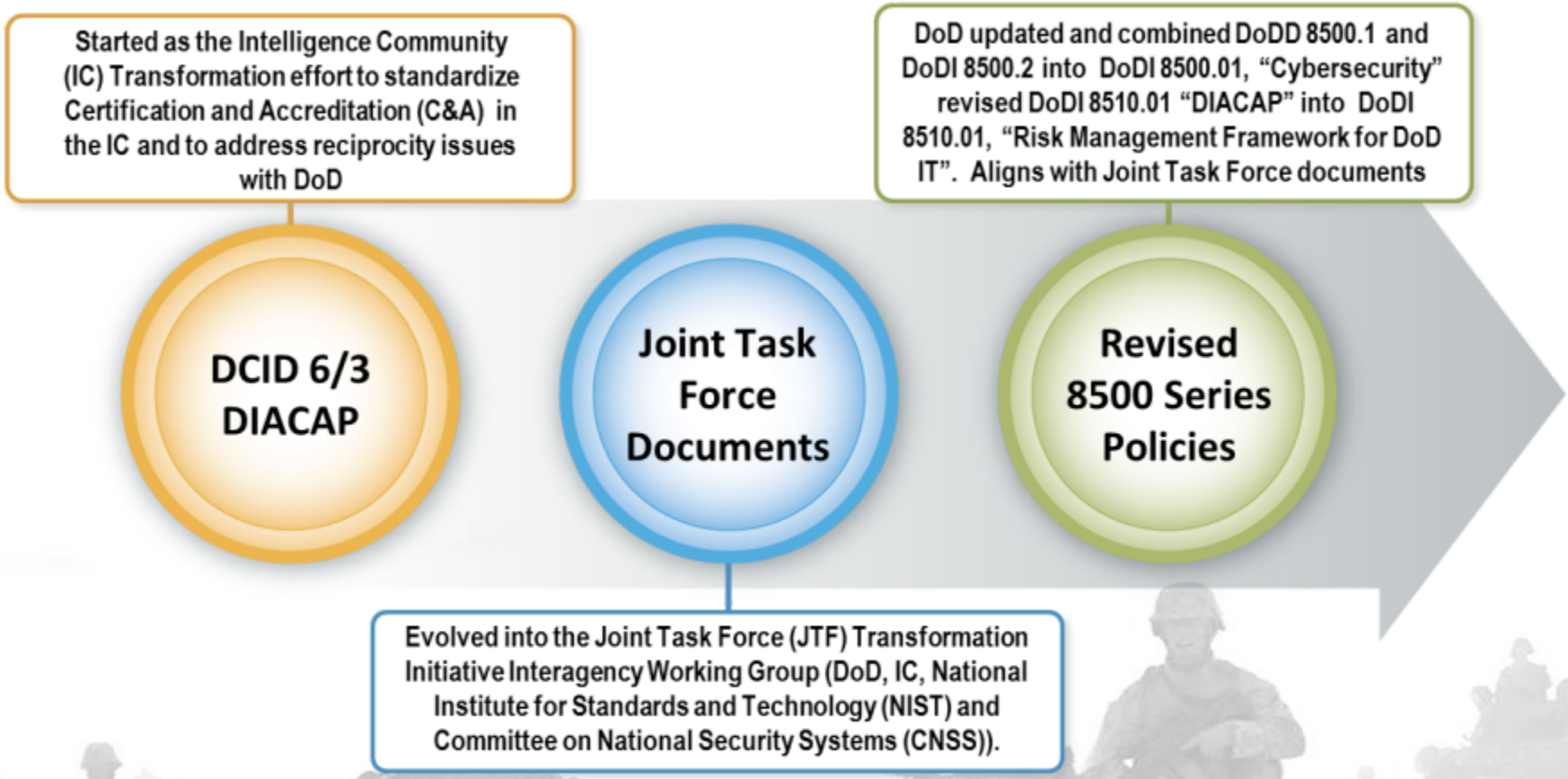
IA for DoD Systems: Transformation from DIACAP to the new Risk Management Framework (RMF) for DoD IT

Mr. Kevin Dulany, CISSP, CISM, CISA, CAP
Chief, Risk Management Oversight Division
Department of Defense (DOD) Chief Information Officer (CIO)
Deputy CIO for Cybersecurity
Cybersecurity Implementation and Integration (CSI&I)

SUPPORT THE WARFIGHTER

Why the Transformation?


Started as the Intelligence Community (IC) Transformation effort to standardize Certification and Accreditation (C&A) in the IC and to address reciprocity issues with DoD
DoD updated and combined DoDD 8500.1 and DoDI 8500.2 into DoDI 8500.01, "Cybersecurity" revised DoDI 8510.01 "DIACAP" into DoDI 8510.01, "Risk Management Framework for DoD IT". Aligns with Joint Task Force documents
DCID 6/3 DIACAP
Joint Task Force Documents
Revised 8500 Series Policies
Evolved into the Joint Task Force (JTF) Transformation Initiative Interagency Working Group (DoD, IC, National Institute for Standards and Technology (NIST) and Committee on National Security Systems (CNSS)).

Transformation Bottom Line – DoD will continue to follow the DoD 8500 series documentation for Cybersecurity policy (formerly Information Assurance)

DoD Leverages and Builds Upon Numerous Existing Federal Policies and Standards - Less DoD Policy to Write and Maintain

DoD participates in development of CNSS and NIST documents ensuring DoD equities are met

DoD leverages CNSS and NIST policies and filters requirements to meet DoD needs

DoD participates in CNSS and NIST policy development as a vested stakeholder with the goals of a more synchronized cybersecurity landscape and to protect the unique requirements of DoD Missions and warfighters

Cybersecurity Policy Alignment

NIST

NIST SP 800-39
Managing Information Security Risk

NIST SP 800-37
Risk Management Framework

NIST SP 800-30
Risk Assessment

NIST SP 800-53
Cybersecurity Controls and Enhancements

NIST SP 800-53A
Cybersecurity Control Assessment Procedures

NIST SP 800-137
Continuous Monitoring

NIST SP 800-60
Mapping Types of Information to Security Categories

NIST SP 800-160 (DRAFT)
Security Engineering Guideline

DoD

DoDI 8500.01 "Cybersecurity"
IT Definitions
Security Controls
Guidance
Enterprise Governance

DoDI 8510.01 "Risk Management Framework for DoD IT"

NSS

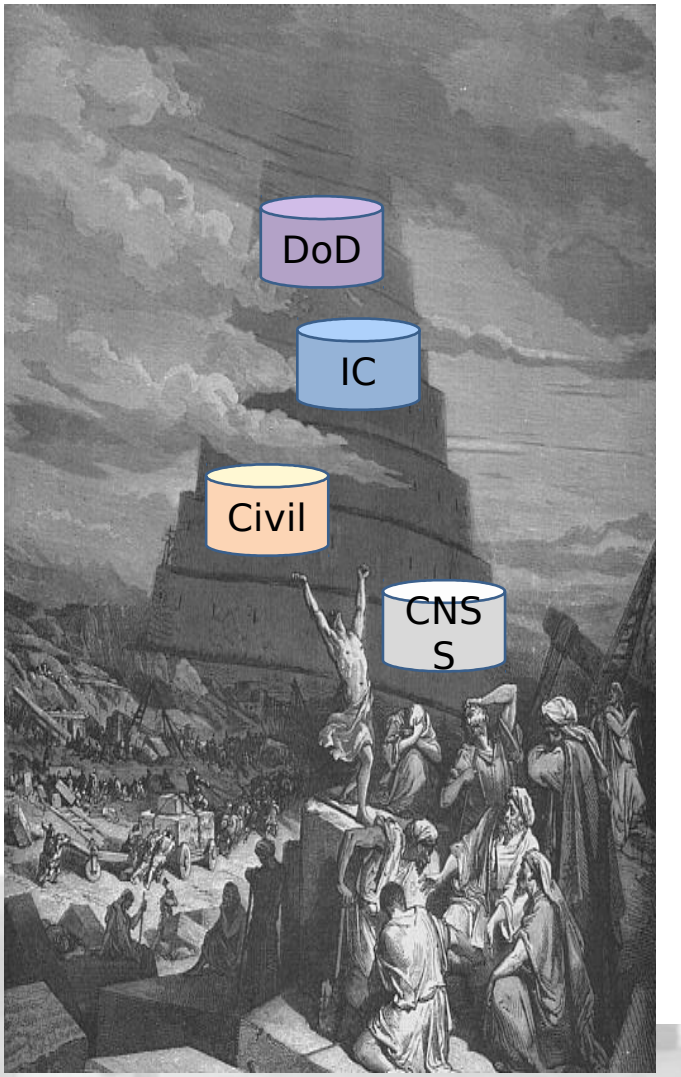
CNSSP 22
IA Risk Management Policy for NSS

CNSSI 1253
Categorization Baselines
NSS Assignment Values

CNSSI 1253A
Implementation and Assessment Procedures

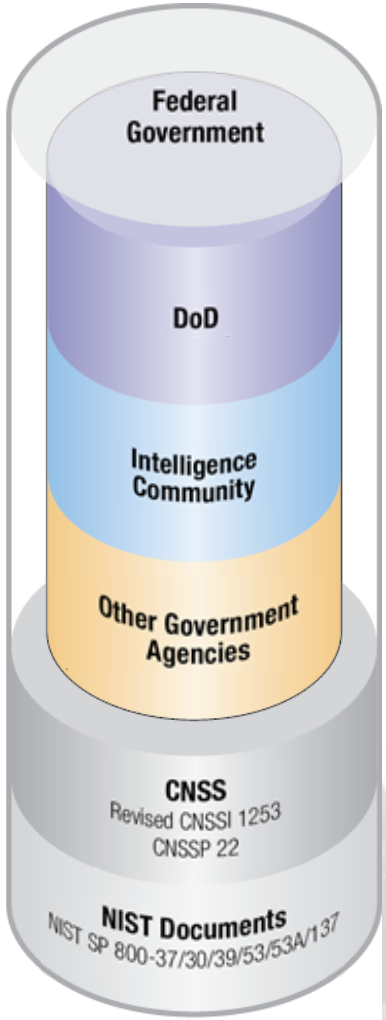
CNSS 4009
Information Assurance/Cybersecurity Definitions

Common Federal cybersecurity terminology so we are all speaking the same language

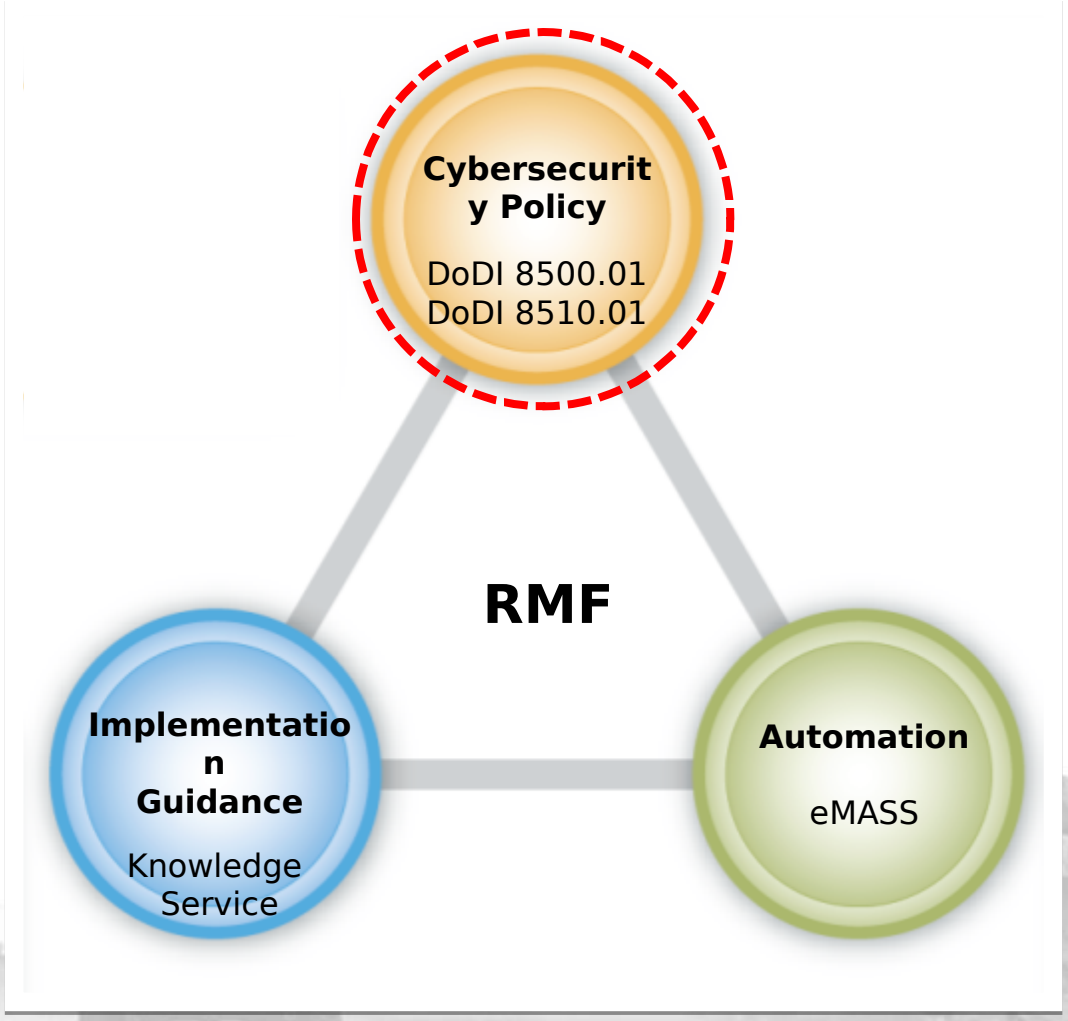


Joint Task Force Transformation Initiative

Streamlines processes and allows for easier interconnection and sharing of information



Successful Execution of DoD Cybersecurity Policy is Enabled Through Three Inter-Related DoD CIO Initiatives



DoD Policy Transformation Highlights

Published Versions DoDD 8500.1, DoDI 8500.2, DoDI 8510.1		Updated Versions DoDI 8500.02, DoDI 8510.01
Information Assurance	Joint Taskforce Transformation Initiative	Cybersecurity
Mission Assurance Category (MAC) / Confidentiality Level (CL)		**Security Objective**: Confidentiality, Integrity, Availability
DoD Specific IA Definitions		**Impact Value**: Low – Moderate – High CNSSI 4009 Glossary for cybersecurity terms
DoD Security Controls		NIST SP 800-53 security control catalog. Uses CNSSI 1253 to categorize and select controls
C&A Process		Risk Management Framework Lifecycle

Cybersecurity Policy Update

DoDI 8500.01 "Cybersecurity"

- Adopts the term "Cybersecurity" in lieu of "Information Assurance"
- Extends applicability to all DoD information technology processing DoD information
- Emphasizes operational resilience, integration, and interoperability
- Aligns with Joint Task Force Transformation Initiative (DoD, NIST, IC, and CNSS)
- Leverages and builds upon numerous existing Federal policies and standards so we have less DoD policy to write and maintain
- Adopts common Federal cybersecurity terminology so we are all speaking the same language
- Transitions to the newly revised NIST SP 800-53 Security Control Catalog
- Incorporates security early and continuously within the acquisition lifecycle

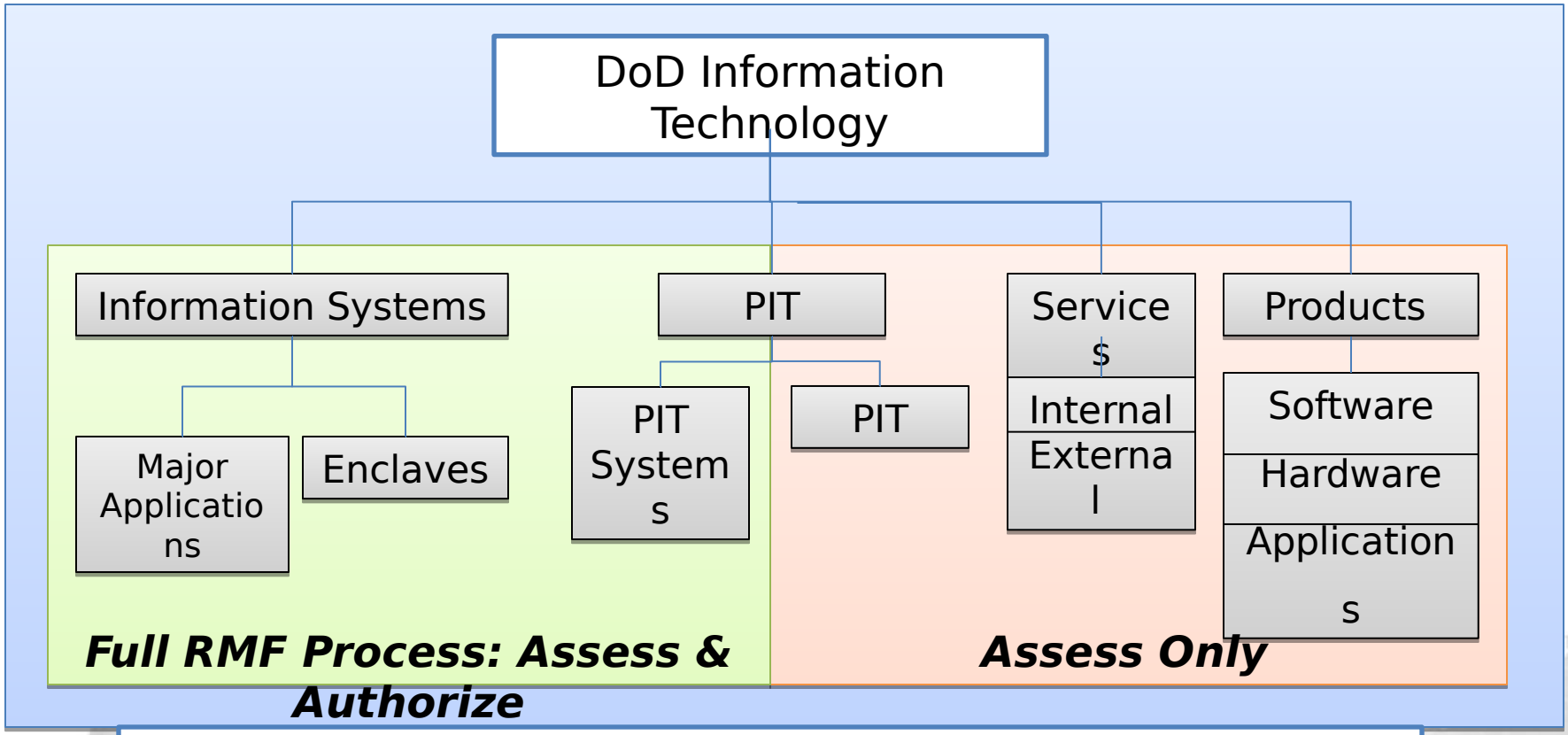
DoDI 8510.01 "Risk Management Framework for DoD Information Technology"

- Adopts NIST's Risk Management Framework, used by Civil and Intelligence communities
- Provides clarity regarding what IT should undergo the RMF process and how
- Supports and promotes enterprise-level authorization of IT systems and services
- Moves from a checklist-driven process to a risk based approach
- Embeds the RMF steps and activities in the DoD Acquisition Lifecycle
- Promotes DT&E and OT&E integration
- Implements cybersecurity via security controls vice numerous policies and memos
- Adopts reciprocity as the norm and codifies reciprocity tenets
- Strengthens enterprise-wide IT governance
- Emphasizes continuous monitoring and timely correction of deficiencies

Status: Documents were approved for signature by DA&M/WHS and are with General Counsel for final legal review. ***Target Publish Date: 2Q FY14***

DoDI 8500.01 "Cybersecurity"

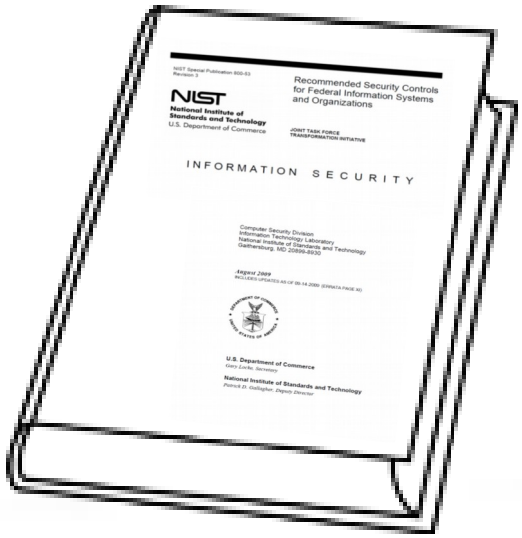
- Extends applicability to all DoD information technology processing DoD information



Cybersecurity applies to all IT that receives, processes, stores, displays, or transmits DoD information

DoDI 8500.01 “Cybersecurity”

- Transitions to the newly revised NIST SP 800-53 Security Control Catalog


NIST
National Institute of Standards and Technology
U.S. Department of Commerce
Recommended Security Controls for Federal Information Systems and Organizations
INFORMATION SECURITY
U.S. Department of Commerce
National Institute of Standards and Technology

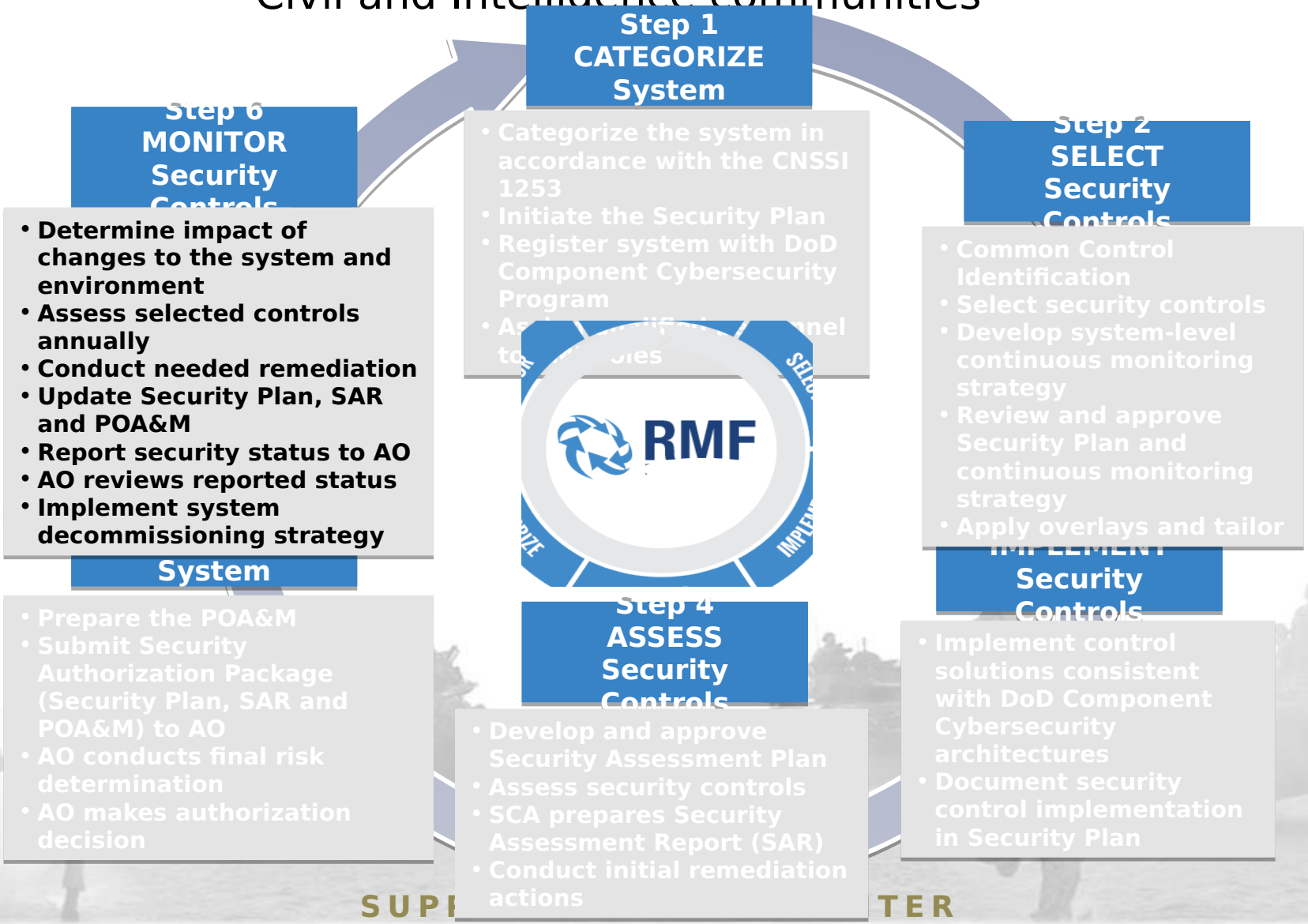
AC-1	Access Control Policy and Procedure
AC-2	Account Management
AT-1	Security Awareness and Training Policy and Procedures
AT-2	Security Awareness
AU-1	Audit and Accountability Policy and Procedures
AU-2	Auditable Events
CA-1	Security Assessment and Authorization Policy and Procedures
CM-1	Configuration Management Policy and Procedures

Major Areas Enhanced By New Security Controls

- Advanced Persistent Threat
- Insider Threat (Removable Media)
- Supply Chain
- Cross Domain
- Identity Management

DoDI 8510.01 "Risk Management Framework for DoD IT"

- Adopts NIST's Risk Management Framework, used by Civil and Intelligence communities


Step 1
CATEGORIZE System
• Categorize the system in accordance with the CNSSI 1253
• Initiate the Security Plan
• Register system with DoD Component Cybersecurity Program
Step 2
SELECT Security Controls
• Common Control Identification
• Select security controls
• Develop system-level continuous monitoring strategy
• Review and approve Security Plan and continuous monitoring strategy
• Apply overlays and tailor
Step 3
IMPLEMENT Security Controls
• Implement control solutions consistent with DoD Component Cybersecurity architectures
• Document security control implementation in Security Plan
Step 4
ASSESS Security Controls
• Develop and approve Security Assessment Plan
• Assess security controls
• SCA prepares Security Assessment Report (SAR)
• Conduct initial remediation actions
Step 5
AUTHORIZE System
• Prepare the POA&M
• Submit Security Authorization Package (Security Plan, SAR and POA&M) to AO
• AO conducts final risk determination
• AO makes authorization decision
Step 6
MONITOR Security Controls
• Determine impact of changes to the system and environment
• Assess selected controls annually
• Conduct needed remediation
• Update Security Plan, SAR and POA&M
• Report security status to AO
• AO reviews reported status
• Implement system decommissioning strategy
RMF

DoDI 8510.01 “Risk Management Framework for DoD IT”

- Moves from a checklist-driven process to a risk based

DIACAP Compliance Check

Are you compliant with these controls?

☐ Yes

☑ No

STOP

Risk Management Framework

Are you compliant with these controls?

☐ Yes

☑ No

What is the **Risk**? Consider:

- Vulnerability Level (includes STIG findings)
- Associated Threats
- Likelihood of Exploitation
- Impact Level (C/I/A)
- Compensating Controls and Mitigations

What is the **Residual Risk**? What is my organization’s risk tolerance? What is my risk tolerance?

Risk Accepted

GO

DoDI 8510.01 "Risk Management Framework for DoD IT"

- Adopts reciprocity as the norm and codifies reciprocity tenets

- **Systems have only a single valid authorization**
- **Applied appropriately, reciprocity reduces redundant testing, assessing and documentation, and the associated costs in time and resources**
- **The DoD RMF presumes acceptance of existing test and assessment results and authorization documentation**
- **DoDI 8510 provides use cases describing the proper application of DoD policy on reciprocity in the most frequently occurring scenarios**

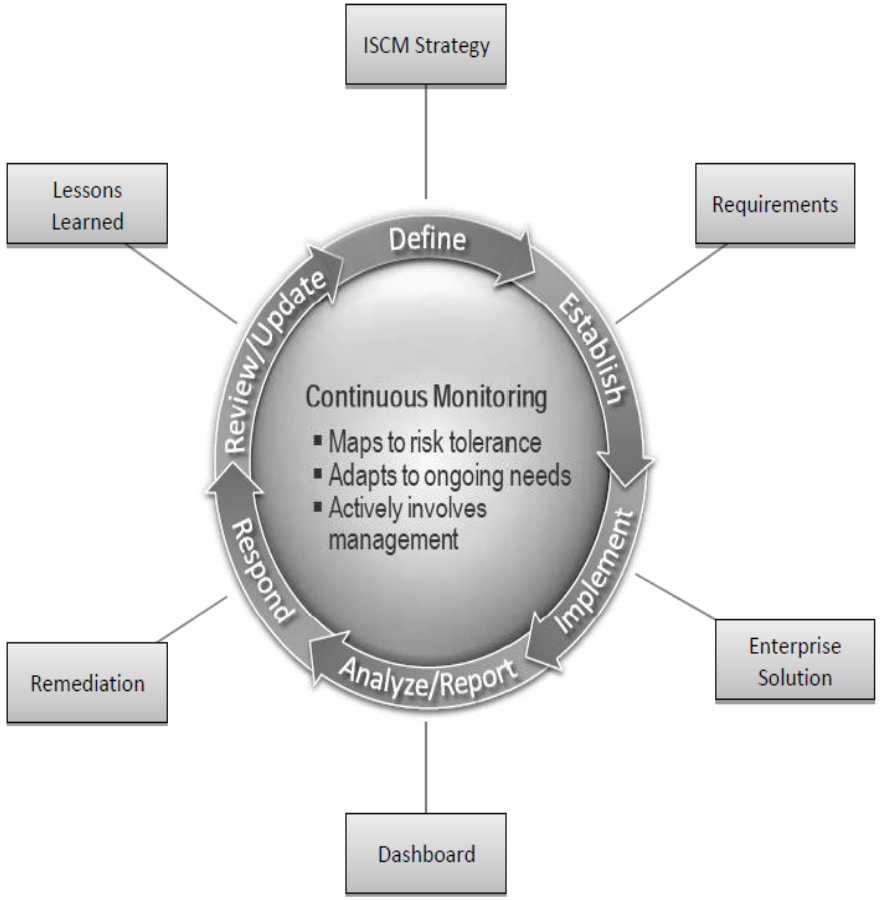
Process for System Acceptance:

1. Review the complete security authorization package
2. Determine the security impact of connecting the deploying system within the receiving enclave or site
3. Determine the risk of hosting the deploying system within the enclave or site
4. If the risk is acceptable, execute a documented agreement between deploying and receiving organizations
5. Document the acceptance by the receiving AO
6. Update the receiving enclave or site authorization documentation for inclusion of the deployed system

DoDI 8510.01 "Risk Management Framework for DoD IT"

- Emphasizes continuous monitoring and timely correction of deficiencies

- RMF is necessary to set the **baseline** for the initial authorization (i.e, meeting CS expectations)
- Developing the programmatics for institutionalizing **ongoing authorization** (vice 3 year reaccreditations) by leveraging a robust Continuous Monitoring Program, and developing joint processes to adopt reciprocity for cybersecurity across DoD the IC, and Federal Civilian Agencies.



CNSSI 1253, "Security Control Categorization and Selection for National Security Systems"

- Required by DoD 8510.01 for all information systems and PIT systems
- Builds on and is a companion document to NIST Special Publication SP 800-53
- Should be used as a tool by ISSEs, AOs, SISOs, Data Owners and others to select and agree upon appropriate protections for an NSS
- Adopts FIPS 199, Categorize NSS using three security objectives (confidentiality, integrity, and availability) with one impact value (low, moderate, or high) for each of the security objectives
- Defines and provides guidance on developing and implementing overlays

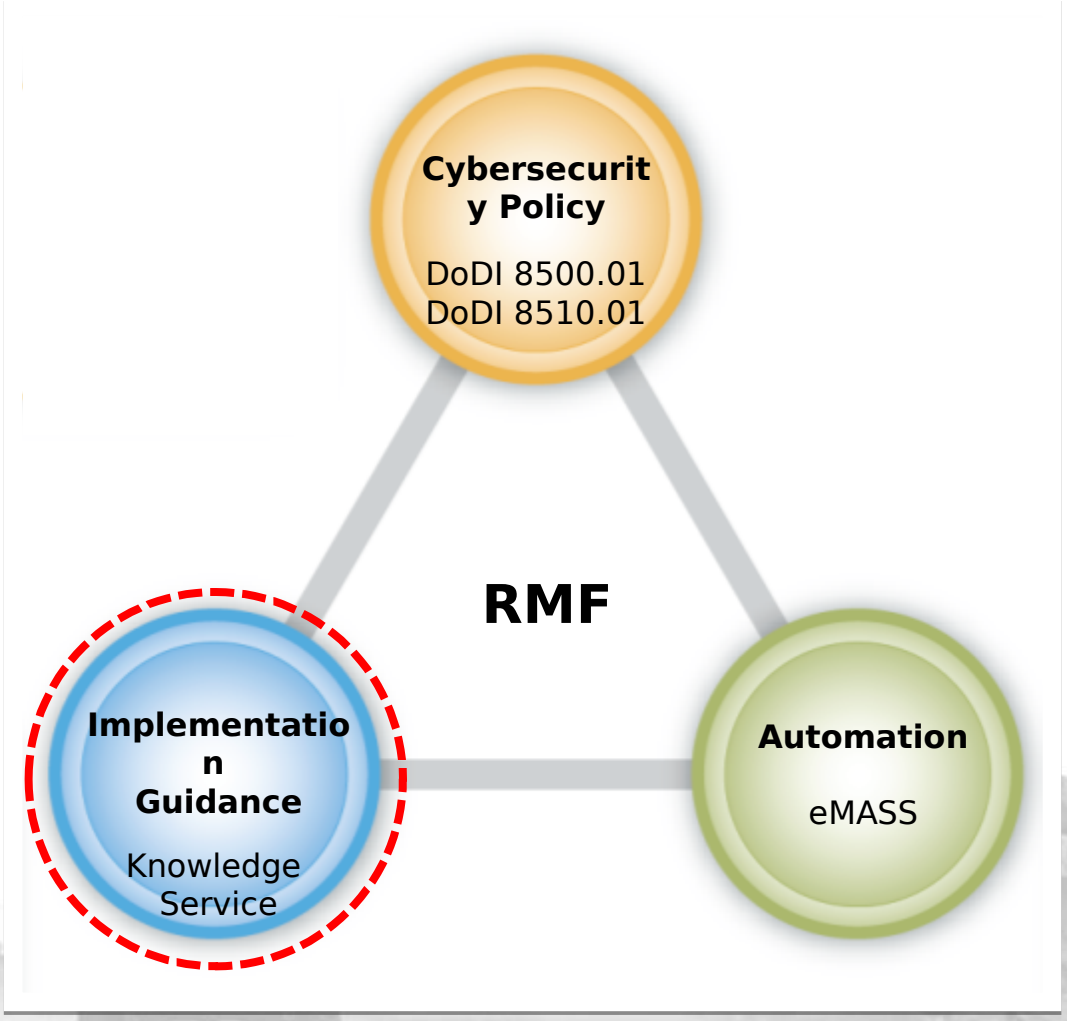
CNSS Overlays

- **Overlays address additional factors beyond impact (baselines only address impact of loss of confidentiality, integrity, and availability)**
- **Enterprise Tailoring**
  - Consistent approach and set of security controls by subject area
  - One time resource expenditure vs. continued expenditures of single system tailoring
  - Promotes reciprocity

CNSS Overlays Status

CNSS Published Overlays	CNSS Overlays in Development (VETTED)	Proposed Overlays (NOT VETTED)
Intelligence (FOUO, Oct 2012) Space Platforms (Jun 2013) Cross Domain Solutions (Sept 2013)	Classified Information Privacy Information Tactical Environment Industrial Control Systems Information Accessibility	**Formally Submitted for Approval** Research Development Test & Evaluation Modeling & Simulation
		Informal Suggestions Cloud DECC/Data Center Nuclear Command and Control Platform IT Mobile/Wireless Networking Medical Systems CUI PKI DoD SAPs

Successful Execution of DoD Cybersecurity Policy is Enabled Through Three Inter-Related DoD CIO Initiatives



DIACAP/RMF Knowledge Service

The Knowledge Service is the **authoritative source** for information, guidance, procedures, and templates on how to execute the DIACAP and Risk Management Framework

https://diacap.iaportal.navy.mil/login.htm

DIACAP/RMF Knowledge Service Overview

- A web-based, DoD PKI-enabled resource
- Developed under the ownership and authority of DoD CIO
- An information repository and collaboration forum for the DIACAP/RMF TAG and corresponding TAG Working Groups
- A collaboration workspace for the DIACAP/RMF user community to develop, share and post lessons learned and best practices
- A library of tools, diagrams, process maps, documents, etc., to support and aid in execution of the DIACAP/RMF
- A source for cybersecurity news and events and other cybersecurity-related information resources

Knowledge Service Updates

- **NIST SP 800-53 Controls explorer (includes CNSSI 1253 baselines and overlays)**
- **Advanced Policy Search Capability**
- **Drafted Over 57 Pages of Online Content to include new information on:**
  - Risk Assessment
  - IT types
  - Control Categorization and Selection
  - Common Controls and Inheritance
- **Key Pages Requiring Community Input (TAG and DAA Summit)**
  - Reciprocity Pages
  - Security Authorization Package Templates
  - Implementation Guidance and Assessment Procedures

RMF Technical Advisory Group (RMF TAG)

- **Mission:** Strengthen and evolve the ability for DoD to rapidly deploy secure IT systems that enable information sharing between the Department, the IC, and other entities.

- **Duties:**
  - Provide implementation guidance for the RMF
  - Provide detailed analysis and authoring support for the enterprise portion of the Knowledge Service (KS)
  - Recommend changes to security controls, baselines, and RMF policy
  - Advise DoD forums established to resolve RMF priorities and cross-cutting issues
  - Develop and manage RMF automation requirements

- **Chair:** DoD SISO appointed

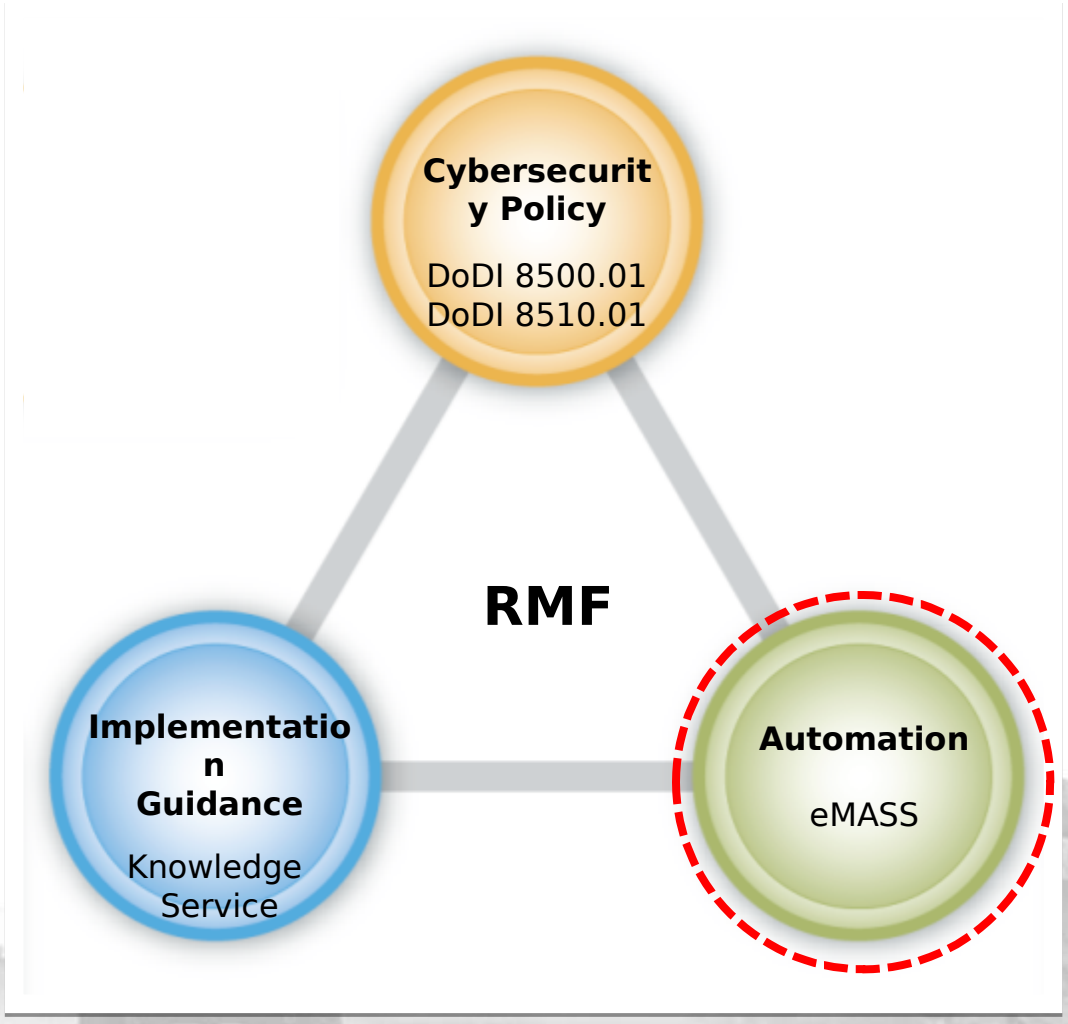
- **Members:** All DoD Components are authorized to be represented by one primary and one alternate cybersecurity SME.

**from draft RMF TAG charter revised for updated DoDI 8510*

Cybersecurity Guidebook for PMs

- **A practical reference for PMs to integrate cybersecurity throughout the acquisition lifecycle**
- **Authoring team chaired by USD(AT&L) and DoD CIO**
  - Participants: DOT&E, Joint Staff, Army, Navy, Marine Corps, Air Force, USCYBERCOM, DISA, NSA and DIA
- **Expect to be published in conjunction with DoDI 8500.01 and DoDI 8510.01**

Successful Execution of DoD Cybersecurity Policy is Enabled Through Three Inter-Related DoD CIO Initiatives



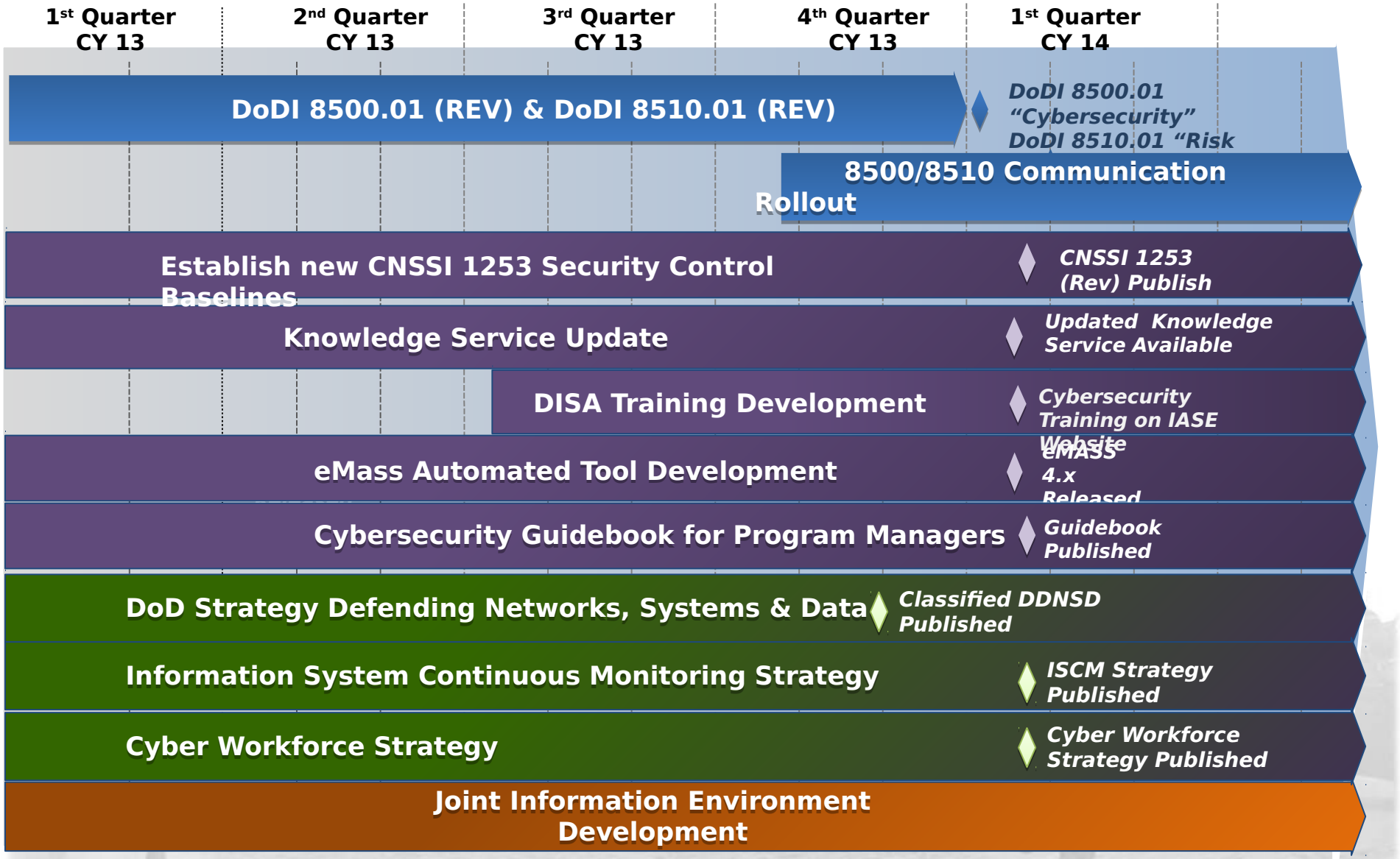
eMASS Overview

- Stands for Enterprise Mission Assurance Support Service
- Establishes a standard approach to: develop, collect, and manage cybersecurity-related data across DoD Organizations
- A GOTS, DISA-Sponsored Enterprise Service owned and centrally managed by DISA PEO-MA
- Currently hosted at the DISA DECC, Columbus, OH, residing on both the NIPR and SIPR Nets
- Allows for customizable organizational taxonomy, workflow, and role-based access to enable efficient workload management and enforce accountability
- Consistently generate all required DIACAP/RMF Deliverables through automated, dynamic report capabilities
- Major version releases every six months

eMASS RMF Releases

- **Initial release for eMASS RMF is planned for deployment in Jan/Feb 2014**
  - ❑ Allow users to create RMF system record / package
  - ❑ Apply NIST 800-53 Rev 4 Security Controls
  - ❑ Manage Security Controls
  - ❑ Initial RMF Package Reports (limited format)
  - ❑ Updates for Capacity Planning and Performance based on increasing data set size and complexity
  - ❑ Limited support for DoD Specific Assignment Values (DSPAV)
- **Future eMASS releases are being coordinated with DoD CIO to support additional RMF guidance and enhancements**
  - ❑ Complete support for DSPAV
  - ❑ Complete support for Overlays
  - ❑ DIACAP to RMF Transition Wizard
  - ❑ RMF GUI Redesign
  - ❑ Official DoD RMF Policy Implementation Guidance
  - ❑ Official DoD RMF Assessment Procedures
  - ❑ Risk Assessment Report and more…

Cybersecurity Efforts


1st Quarter CY 13
2nd Quarter CY 13
3rd Quarter CY 13
4th Quarter CY 13
1st Quarter CY 14
DoDI 8500.01 (REV) & DoDI 8510.01 (REV)
DoDI 8500.01 "Cybersecurity"
DoDI 8510.01 "Risk
8500/8510 Communication Rollout
Establish new CNSSI 1253 Security Control Baselines
CNSSI 1253 (Rev) Publish
Knowledge Service Update
Updated Knowledge Service Available
DISA Training Development
Cybersecurity Training on IASE Website
eMass Automated Tool Development
eMASS 4.x Released
Cybersecurity Guidebook for Program Managers
Guidebook Published
DoD Strategy Defending Networks, Systems & Data
Classified DDNSD Published
Information System Continuous Monitoring Strategy
ISCM Strategy Published
Cyber Workforce Strategy
Cyber Workforce Strategy Published
Joint Information Environment Development

Questions/Wrap Up

Mr. Kevin M. Dulany
Chief, Risk Management Oversight Division
DOD–CIO, DCIO–Cybersecurity, CSI&I
Office: (571) 372–4699
Kevin.M.Dulany.civ@mail.mil

BACKUP

RMF Transition Timeline per DoDI 8510.01, Enclosure 8

System Authorization Status		Transition Timeline And Instructions
1	New start or unaccredited	Transition to the RMF within six months
2	System has initiated DIACAP but has not yet started executing the DIACAP Implementation Plan	Transition to the RMF within six months
3	System has begun executing the DIACAP Implementation Plan	Either: a. Develop a strategy and schedule for transitioning to the RMF not to exceed the system re-authorization timeline or, b. Transition to the RMF within six months
4	System has a current valid DIACAP accreditation decision	Develop a strategy and schedule for transitioning to the RMF not to exceed the system re-authorization timeline
5	System has a DIACAP accreditation that is more than 3 years old	Transition to the RMF within six months

Sources for DoD Policy

IA Support Environment

http://iase.disa.mil/index2.html

Knowledge Service

https://diacap.iaportal.navy.mil/login.htm

DoD Issuances Website

http://www.dtic.mil/whs/directives/index.html

CNSS Policies

http://www.cnss.gov/policies.html

NIST Publications

http://csrc.nist.gov/publications/PubsSPs.html

IATAC DoD IA Policy Chart

http://iac.dtic.mil/csiac/ia_policychart.html

C&A Transformation Goals

1. Define a ***common set of trust (impact) levels*** and adopt and apply them across the Intelligence Community (IC) and DoD. Organizations will no longer use different levels with different names based on different criteria.
2. Adopt ***reciprocity*** as the norm, enabling organizations to accept the approvals by others without retesting or reviewing.
3. Define, document, and adopt ***common security controls***, using NIST Special Publication (SP) 800-53 as a baseline.
4. Adopt a ***common lexicon***, using CNSS Instruction 4009 as a baseline thereby providing DoD and IC a common language and common understanding.
5. Institute a ***senior risk executive function***, which bases decisions on ***an "enterprise" view of risk considering all factors***, including mission, IT, budget, and security.
6. Incorporate information assurance (IA) into ***Enterprise Architectures*** and deliver IA as ***common enterprise services*** across the IC and DoD.
7. Enable a ***common process*** that incorporates security within the ***"lifecycle"*** processes and eliminate security-specific processes. The common process will be adaptable to various development environments.